

**Verizon New England Inc.  
d/b/a Verizon Massachusetts**

**Commonwealth of Massachusetts**

**D.T.E. 02-8**

**Respondent:** Lawrence R. Craft

**Title:** Manager

**REQUEST:** Allegiance Telecom of Massachusetts, Inc., Set #2

**DATED:** June 5, 2002

**ITEM:** AL-VZ 2-1 In your response to AL-VZ-1-24, you state:

**“The following security measures were taken Company-wide since September 11<sup>th</sup>:**

- ?? Company facility protection was greatly increased
- ?? 24 X 7 guard coverage was instituted at certain critical locations
- ?? Guard force was upgraded at critical locations, *i.e.*, experience levels of guards
- ?? Armed guards were posted at certain critical facilities
- ?? Supervision of guard force was upgraded
- ?? Verizon Security personnel were assigned to critical buildings to oversee security and perform security reviews (approximately 1,000 locations visited per week)
- ?? Access control at Verizon facilities was strengthened/reinforced
- ?? Verizon IDs were scrutinized
- ?? Bag, parcel searches were conducted
- ?? Visible Verizon ID badge policy was enforced, and employees were encouraged to challenge personnel without visible IDs
- ?? Mail Security Guidelines were developed and implemented
- ?? Response protocol was developed

For each measure listed above, please provide the following:

- (a) The approximate cost of implementing the measure, on whatever basis such information is available or ascertainable through reasonable efforts (e.g., per central office, per state, per Verizon region, or for the company as a whole);

**ITEM: AL-VZ 2-1**

- (b) The approximate cost of implementing the measure in Massachusetts;
- (c) A description of how Verizon is recovering or plans to recover the costs it incurs in taking each measure;
- (d) The name of the Verizon employee primarily responsible for implementing each measure in Massachusetts;
- (e) Any and all documents related to the implementation of each measure;
- (f) A description of any metrics or other criteria Verizon has adopted or plans to adopt to assess its success in implementing each measure and, to the extent any data related to such metrics or other criteria has been generated, produce copies of such data;
- (g) The critical locations in Massachusetts at which 24 X 7 guard coverage was instituted;
- (h) The critical buildings in Massachusetts to which Verizon security personnel were assigned to oversee security and perform security reviews and the results of any such reviews.

**REPLY:**

- (a) Verizon MA has not tracked the costs associated with the various security measures adopted since September 11, 2001. Verizon MA has also not sought to recover such costs from other carriers through collocation-related rates. Verizon MA enhanced its security measures based on the critical need to safeguard its network to ensure public safety - not based on a cost/benefit approach..The requested information is not available.
- (b) The requested information is not available.
- (c) There are no specific plans for recovery of these costs. See also Verizon MA's Reply to (a) above.
- (d) There was no one person primarily responsible as it was a multi-district initiative under the general direction of Verizon's Security Department.
- (e) Specific security guidelines relating to mail and toxic emissions were developed as a result of September 11, 2001. Verizon MA considers those documents highly proprietary, commercially

sensitive information. Accordingly, Verizon MA will provide such information to the Department only and to parties subject to the terms of a suitable Protective Agreement.

- (f) Specific metrics or quantitative data were not used to evaluate the effectiveness of these temporary measures. See Verizon MA's Reply to (h) below.
- (g) Verizon MA added security guards on a 24 hour, seven-day per week basis at two additional CO locations (Braintree and Brockton) in Massachusetts after September 11<sup>th</sup>.
- (h) Verizon MA objects to this request on the grounds that it is unreasonable because of the overly broad scope of the data requested and the burden of compliance. Verizon MA also objects to this request on the grounds that it seeks information that is confidential in nature and is irrelevant, immaterial, and not reasonably calculated to lead to the discovery of admissible evidence. Verizon MA further objects to the request because it seeks highly proprietary, commercially sensitive and security-related information on a central-office specific basis.

Without waiving these objections, Verizon MA responds to this request as follows:

The requested information is voluminous. Due to the voluminous nature of the requested information, a copy of all documents will be made available for inspection by the Department and other parties at the Company's offices at 125 High Street Boston, Massachusetts, at a mutually agreeable time. In addition, because of the confidential nature of the documents requested, Verizon MA will provide such information to the Department only and to parties subject to the terms of a suitable Protective Agreement.

**Verizon New England Inc.  
d/b/a Verizon Massachusetts**

**Commonwealth of Massachusetts**

**D.T.E. 02-8**

**Respondent:** Peter Shepherd

**Title:** Director

**REQUEST:** Allegiance Telecom of Massachusetts, Inc., Set #2

**DATED:** June 5, 2002

**ITEM:** AL-VZ 2-2 In AL-VZ-1-23, in response to the question "Does Verizon believe that any cost/benefit analysis should be applied to the proposed measures," Verizon responded "No."

- (a) If the benefits of a measure as compared to its cost should not be a factor in the Department's consideration of additional security measures, what criteria do you believe the Department should apply in choosing among various proposals that might be presented to it in this proceeding?
- (b) If Verizon does not believe cost/benefit analysis should be used with respect to security measures, is it Verizon's position that it has already implemented all technically feasible security measures in its Massachusetts central offices? If Verizon has not implemented all technically feasible security measures in its Massachusetts central offices, please identify each such technically feasible security measure that has not been implemented and, for each, state the reason that measure has not been implemented.

**REPLY:**

- (a) In assessing the proposed security measures for collocated central offices ("COs"), the Department should consider whether a CO is critical based on certain factors, as stated in Verizon MA's Surrebuttal Testimony (pp. 14-17). Because there is a greater risk of potential harm to the telecommunications network if there is a security violation in so-called "critical" offices, those COs should be afforded heightened security protection. By designating critical COs as "virtual collocation only" and denying access to those COs, the increased security risks are reasonably minimized.

In all other collocated COs, the Department should maintain the existing security measures adopted by Verizon MA in Massachusetts. They consist of a combination of established security methods (*e.g.*, electronic card reader systems, identification badges, etc.), as well as a continuation of Verizon MA's existing collocation policies (*e.g.*, separate and segregated space, separate pathways, etc.). Verizon MA also plans to enhance and expand its use of the above security methods as described in its testimonies. In addition, the Department should consider the heightened security risks inherent in remote terminal locations - and the impracticability of other security measures - in determining that an escort requirement is appropriate under those circumstances. *See e.g.*, Verizon MA's Surrebuttal Testimony, at 12-13.

- (b) While a proposed security measure must be technically feasible to consider implementing it in a collocated central office ("CO"), that is certainly not the only consideration, as explained (a) above and in Verizon MA's testimonies. Those technically feasible security methods raised in this proceeding that have not been implemented by Verizon MA are discussed in Verizon MA's Replies to AL-VA 2-4 and AL-VZ 2-7, as well as in Verizon MA's testimonies.

**Verizon New England Inc.  
d/b/a Verizon Massachusetts**

**Commonwealth of Massachusetts**

**D.T.E. 02-8**

**Respondent:** Peter Shepherd

**Title:** Director

**REQUEST:** Allegiance Telecom of Massachusetts, Inc., Set #2

**DATED:** June 5, 2002

**ITEM:** AL-VZ 2-3 In response to XO-VZ-1-4, Verizon states:

“The preliminary criteria described in Verizon MA’s panel testimony is intended as the basis for the Department and the Company to develop a framework for identifying those critical offices. Verizon MA anticipates that a small number of COs (e.g., only a handful) would be designated as critical.”

Is it Verizon’s position that a CO could be designated as critical based solely on the identity and nature of a Verizon customer or customers served from that CO?

**REPLY:** It is possible that the Department may determine that a central office (“CO”) should be deemed “critical” based on the customer(s) served from that CO and the nature of their business, *i.e.*, whether they provide for the public’s health, safety, welfare and/or protect the nation’s security interests.

VZ # 151

**Verizon New England Inc.  
d/b/a Verizon Massachusetts**

**Commonwealth of Massachusetts**

**D.T.E. 02-8**

**Respondent:** Lawrence R. Craft  
**Title:** Manager

**REQUEST:** Allegiance Telecom of Massachusetts, Inc., Set #2

**DATED:** June 5, 2002

**ITEM:** AL-VZ 2-4 Is the use of biometric feedback devices to authenticate access authority technically feasible in any Massachusetts central office in which CLECs are currently collocated? If so, why have such devices not been installed in those central offices?

Biometric devices (*e.g.*, fingerprint detector, signature analyzer, retinal scanner, or voice recognition equipment) are probably technically feasible in Verizon MA' collocated central offices ("COs") provided that the necessary hardware and software and database systems used to match individual physical characteristics are deployed. However, biometric devices are neither practical nor reliable security measures at this time.

First, they can only compare the features of individuals scanned with profiles stored in a specific database. Second, they can produce inaccurate scanning results (*e.g.*, false positives), or the system can be fooled by latent prints (*i.e.*, when someone lifts a fingerprint image from a surface and then uses it) or physical disguises. Third, biometric devices can be slower than standard access system methods, such as electronic card readers, and, in some cases, are prone to malfunction. For instance, thumbprint or hand scanner surfaces must be kept clean and free of body oils and other debris build-up to function properly.

It is Verizon's understanding that pilot programs and trials are underway to improve the accuracy and reliability of biometric devices. Until further testing is conducted and the value and effectiveness of these devices are proven, it would not be prudent to invest in biometric technology. In addition, biometric devices may be considered invasive, thereby raising serious privacy concerns.

**Verizon New England Inc.  
d/b/a Verizon Massachusetts**

**Commonwealth of Massachusetts**

**D.T.E. 02-8**

**Respondent:** Lawrence R. Craft  
**Title:** Manager

**REQUEST:** Allegiance Telecom of Massachusetts, Inc., Set #2

**DATED:** June 5, 2002

**ITEM:** AL-VZ 2-5 Is there any device or security measure of which Verizon is aware that would alert Verizon to the presence of a door to a secure area in a central office that has been improperly propped open (whether by CLEC or Verizon personnel or vendors)? If so, please identify such device or security measure and state whether it would be technically feasible to install such device or implement such security measure in any Massachusetts central office in which CLECs are currently collocated. If such a device or security measure does exist and it would be technically feasible to install such device or implement such security measure in any Massachusetts central office in which CLECs are currently collocated, please state whether the device or security measure has, in fact, been installed or implemented in any Massachusetts central office. If not, please state why such device or security measure has not been installed or implemented in any Massachusetts central office.

**REPLY:** Verizon MA is aware of door contacts that identify when a specific door is not closed tightly, and has generally deployed those devices on perimeter doors to the central office. Verizon MA also installs door contacts as a standard practice when upgrading to electronic card access systems.

VZ # 153



**Verizon New England Inc.  
d/b/a Verizon Massachusetts**

**Commonwealth of Massachusetts**

**D.T.E. 02-8**

**Respondent:** Lawrence R. Craft

**Title:** Manager

**REQUEST:** Allegiance Telecom of Massachusetts, Inc., Set #2

**DATED:** June 5, 2002

**ITEM:** AL-VZ 2-6 Is there any device or security measure of which Verizon is aware that would prevent former Verizon employees from using an ID or access card to gain unauthorized access to a central office after his or her Verizon employment has ended? If so, please identify such device or security measure and state whether it would be technically feasible to install such device or implement such security measure in any Massachusetts central office in which CLECs are currently collocated. If such a device or security measure does exist and it would be technically feasible to install such device or implement such security measure in any Massachusetts central office in which CLECs are currently collocated, please state whether the device or security measure has, in fact, been installed or implemented in any Massachusetts central office. If not, please state why such device or security measure has not been installed or implemented in any Massachusetts central office.

**REPLY:** Verizon MA's policy is that an employee must return his/her identification badge to his/her supervisor immediately upon the employee's last day of physical presence on the job. Electronic access cards are also returned at the same time and/or inactivated. These security measures prevent former Verizon MA employees from gaining unauthorized access after employment has ended.

VZ # 154

**Verizon New England Inc.  
d/b/a Verizon Massachusetts**

**Commonwealth of Massachusetts**

**D.T.E. 02-8**

**Respondent:** Lawrence R. Craft

**Title:** Manager

**REQUEST:** Allegiance Telecom of Massachusetts, Inc., Set #2

**DATED:** June 5, 2002

**ITEM:** AL-VZ 2-7 Is there any device or security measure of which Verizon is aware that would prevent employees (whether Verizon or CLEC) or vendors from engaging in the practice described in Verizon's panel testimony as "tailgating?" If so, please identify such device or security measure and state whether it would be technically feasible to install such device or implement such security measure in any Massachusetts central office in which CLECs are currently collocated. If such a device or security measure does exist and it would be technically feasible to install such device or implement such security measure in any Massachusetts central office in which CLECs are currently collocated, please state whether the device or security measure has, in fact, been installed or implemented in any Massachusetts central office. If not, please state why such device or security measure has not been installed or implemented in any Massachusetts central office.

**REPLY:** Verizon MA is aware of two devices – turnstiles and mantraps – that may be utilized to deter tailgating. Turnstiles are a barrier type of device that only permit one person at a time to pass through an opening upon that person activating the device with an authorized electronic access card. Mantraps provide a similar function by providing a full barrier in front of and behind the person with only enough space for one person in between the barriers. Both barriers must be activated independently, or in sequence by an authorized electronic access card.

Verizon MA does not believe that either of these methods are feasible or practical in Massachusetts. Sufficient additional space is required to install turnstiles and mantraps in a location. In addition, unless guarded, single-arm turnstiles can be bypassed by simply climbing over them. Multi-bar or gated turnstiles and mantraps would also

**REPLY:** AL-VZ 2-7  
con't.

- 2 -

impede technicians attempting to pass through with bulky supplies, test set gear or tools. For these reasons, Verizon MA has not implemented either of these measures in its Massachusetts central offices.

VZ # 155

**Verizon New England Inc.  
d/b/a Verizon Massachusetts**

**Commonwealth of Massachusetts**

**D.T.E. 02-8**

**Respondent:** Lynelle Reney  
**Title:** Director

**REQUEST:** Allegiance Telecom of Massachusetts, Inc., Set #2

**DATED:** June 5, 2002

**ITEM:** AL-VZ 2-8 If Verizon's proposals as set forth in its Panel Testimony were adopted by the Department, would the following statements be true or false. If any statement is false, in whole or in part, please state why it is false.

- (b) If a CLEC requests physical collocation in a central office, and there is no separate, secure space available for such physical collocation, the CLEC's request for physical collocation would be denied.
- (b) If a CLEC requests physical collocation in a central office, and there is separate secure space available for such physical collocation but no route by which the CLEC can gain access to that space without entering secure Verizon space, the CLEC's request for physical collocation would be denied.

**REPLY:**

- (a) False, in part. Verizon MA would evaluate the request to determine if there was existing, separate and secure space and, if not, it would determine if separate and secured space could be provisioned in order to meet the request. A request would not automatically be denied if there was no existing separate space provided that additional separate and secure space could be made available.
- (b) False. These determinations can only be made on a case-by-case basis, subject to a physical inspection of the central office. There may be alternative routes or separate entrances that can be constructed to meet the request.

**Verizon New England Inc.  
d/b/a Verizon Massachusetts**

**Commonwealth of Massachusetts**

**D.T.E. 02-8**

**Respondent:** Lawrence R. Craft  
**Title:** Manager

**REQUEST:** Allegiance Telecom of Massachusetts, Inc., Set #2

**DATED:** June 5, 2002

**ITEM:** AL-VZ 2-9 In response to AL-VZ-24, Verizon states that since September 11, 2001, on a Company-wide basis Verizon has added "24 X 7 guard coverage" at certain critical locations. In its supplemental response to AL-VZ-1-4, Verizon indicates that it uses security guards at 7 locations in Boston and Cambridge.

- (a) Please indicate when Verizon first began using guards at the 7 locations listed in its supplemental response to AL-VZ-1-4.
- (b) Please indicate whether the post-September 11<sup>th</sup> "24X7 guard coverage" described in Verizon's response to AL-VZ-24 refers to facilities in Massachusetts other than the 7 facilities listed in Verizon's supplemental response to AL-VZ-1-4. If so, please indicate how many Verizon facilities in Massachusetts – other than the 7 facilities listed in Verizon's supplemental response to AL-VZ-1-4 – were staffed by "24X7" security guards after September 11<sup>th</sup> and how many of those Massachusetts facilities still use "24X7" security guards today.

- REPLY:**
- (a) Contract guards at these locations have been used for at least the last three years, although not necessarily on a 24 x 7 coverage basis.
  - (b) See Verizon MA's Reply to 2-1(g). The two additional locations no longer have "24X7" guards.

**Verizon New England Inc.  
d/b/a Verizon Massachusetts**

**Commonwealth of Massachusetts**

**D.T.E. 02-8**

**Respondent:** Lawrence R. Craft  
**Title:** Manager

**REQUEST:** Allegiance Telecom of Massachusetts, Inc., Set #2

**DATED:** June 5, 2002

**ITEM:** AL-VZ 2-10 In Verizon's supplemental response to AL-VZ-1-4, Verizon states that "although security guards may not be assigned to other Massachusetts COs, Verizon technicians are present in the collocated COs." Please indicate if the Verizon technicians described in this supplemental response fulfill all or part of the role of security guards present in other facilities, and, if so, how. Also, are any of the collocated COs where Verizon technicians, but not security guards, are present still considered "unmanned" as that term is defined in Verizon's collocation guidelines (i.e., "An unmanned building is any VZ central location that does not have a permanent employee assigned between the hours of 8am –5pm, Monday through Friday")?

**REPLY:** The technicians do not fulfill all of the roles of a security guard. Verizon technicians are required to verify that individuals are displaying a Verizon-issued Identification card, and challenge or report those individuals who do not comply with that procedure. A central office ("CO") is unmanned if a permanent employee is not assigned to that CO between the hours of 8am and 5pm, Monday through Friday. This is true even though a Verizon technician may have been dispatched to and is temporarily working on the premises.

VZ # 158